CB-BEITRAG

Ondřej Zapletal und Lukas Tatge

Generative Künstliche Intelligenz für KMUs und rechtliche Herausforderungen bei deren Einsatz in China

Aufgrund des starken Wettbewerbsdrucks und anderen marktspezifischen Herausforderungen in China ist es für deutsche Mittelständler essentiell, sich auch vor Ort im chinesischen Markt mit Künstlicher Intelligenz (KI) auseinanderzusetzen, ein umfassendes Know-how in ihren Teams aufzubauen und in Zukunft chinesische generative KI-Technologie in ihre Aktivitäten in China einzubinden. Für ihre Tochtergesellschaften in China stellt sich zusätzlich die Frage, ob und inwieweit es technisch und rechtlich möglich ist, ausländische KI-Modelle nach China zu übertragen. Vor diesem Hintergrund untersucht der Beitrag die technische und rechtliche Landschaft der generativen KI auf dem chinesischen Festland, um deutsche KMU bei der Anwendung von KI in China zu begleiten und zu unterstützen.

I. Einleitung

China hat sich neben den USA als globaler Marktführer im Bereich der generativen KI etabliert und trägt zu etwa 40% der weltweit veröffentlichten generativen KI-Modelle bei. Die strengen regulatorischen Beschränkungen für ausländische generative KI-Modelle haben die Entwicklung diverser inländischer Modelle in China beschleunigt. Diese chinesischen Modelle sind den US-Modellen bei der Bewältigung komplexer Aufgaben in der chinesischen Sprache oft überlegen, insbesondere wenn technische Begriffe und industrielle Zusammenhänge eine wichtige Rolle spielen.

Generative KI dient als starker Katalysator für Innovationen, insbesondere für kleine und mittelständische Unternehmen (KMUs), da diese nun die hochentwickelten KI-Modelle sicher und effizient in ihre Prozesse und Produkte integrieren können.

Anwendungsbereiche sind beispielsweise Prozessoptimierung, Wissensmanagement, technischer Support und weitere komplexen Anwendungen. Der Fokus liegt hierbei meist auf Kosteneinsparungen, indem manuelle und wiederkehrende digitale Prozesse unterstützt oder automatisiert werden, wobei gleichzeitig auch Umsatzsteigerung erreicht werden kann, wenn beispielsweise Verkaufsmitarbeiter von administrativen Aufgaben entlastet werden und sich voll auf den eigentlichen Verkaufsprozess konzentrieren können.

Chinesische Unternehmen haben die Vorteile der generativen KI bereits erkannt. Nach einer neuen Studie des SAS Instituts[1] nutzten 83% der Unternehmen in China generative KI im Verkauf, Marketing, Produktion als auch anderen Bereichen. Da viele deutsche KMU nicht nur in China, sondern auch auf anderen Märkten einem harten Wettbewerb ausgesetzt sind, erwägen viele den Einsatz dieses neuen Werkzeugs, um ihren wirtschaftlichen und technologischen Vorsprung zu sichern. Einige von ihnen haben bereits mit Testanwendungen begonnen.

II. Einführung in Generative KI

Seit Jahrzehnten entwickelt sich der Bereich der Künstlichen Intelligenz (KI) kontinuierlich weiter, getrieben von immer neuen Konzepten und innovativen Ansätzen. Das übergeordnete Ziel ist dabei stets, menschliches Verhalten und Entscheidungen nachzuahmen sowie operative Entscheidungen zu optimieren.

Generative KI-Modelle, die auf der Architektur von neuronalen Netzen basieren und somit nach dem Vorbild des menschlichen Gehirns strukturiert sind, werden mit sehr großen Trainingsdatensätzen trainiert. Sie sind anschließend in der Lage, eigenständig neue Inhalte wie Texte, Bilder und Videos zu erstellen oder interaktive Dialoge mit Nutzern zu führen. Es gibt unterschiedliche Arten von Modelltypen, die sich in ihrer Trainingsweise und Struktur unterscheiden. Am häufigsten werden aktuell transformatorbasierte Modelle (GPT) verwendet, die vor allem für die Textgenerierung genutzt werden. Ein Beispiel dafür ist ChatGPT von OpenAI, das technisch so funktioniert, dass das Modell immer nur das nächste Wort eines Satzes auf der Basis von Wahrscheinlichkeiten vorhersagt. Da diese generativen KI-Modelle mit einer sehr hohen Anzahl an früheren Textbeispielen trainiert wurden, sind sie in der Lage, durch das Auswählen des jeweils wahrscheinlichsten nächsten Wortes einen kohärenten und kontextuell passenden Antworttext zu erzeugen.

Das Besondere und Neue an diesen generativen Modellen ist, dass ein einziges Modell durch seine Größe und generalistische Ausrichtung für unterschiedlichste Aufgaben wie die Erstellung eines Marketingtexts, die Programmierung eines industriellen Roboters oder die Analyse von

1 Studie des SAS Instituts vom 9.7.2024: https://www.sas.com/de_de/news/press-releases/2024/july/genai-research-study-global.html.

Verkaufszahlen eingesetzt werden kann. Dies bietet vor allem KMUs die Chance, führende KI-Modelle sehr schnell und einfach in ihre Prozesse zu integrieren, ohne eigene Entwicklungsressourcen aufbringen zu müssen.
Insbesondere manuelle und wiederkehrende digitale Prozesse können zukünftig durch generative KI-Modelle unterstützt oder sogar ersetzt werden. Mitarbeiter in allen Abteilungen werden generative KI-basierte Anwendungen als Werkzeuge nutzen, um effizienter zu arbeiten, Flüchtigkeitsfehler zu vermeiden und freie Ressourcen für andere Aufgaben zu verwenden. Durch den Einsatz generativer KI sind Unternehmen in der Lage bereits kurz- bis mittelfristig signifikante Kosteneinsparungen zu realisieren.
Generative KI-Anwendungen werden meist so gestaltet, dass die zugrunde liegenden generativen KI-Basismodelle mit nur minimalen Anpassungen ausgetauscht und auf neue, leistungsstärkere Modelle aktualisiert werden können. So vermeiden Unternehmen, in generative KI-Anwendungen zu investieren, die zukünftig nicht mehr genutzt werden können.

III. Übersicht über den generativen KI-Markt in China

KI-Technologie wird in China seit 2016 von höchster Stelle in der Zentralregierung unterstützt und als Schlüsseltechnologie zur Modernisierung der Realwirtschaft angesehen. Nach dem Durchbruch der generativen KI durch OpenAI in den USA wurde diese Technologie in China schnell als eine neue Kerntechnologie definiert. Dies sieht man in der Realwirtschaft durch einen sofortigen Anstieg der privaten und staatlichen Investitionen und Subventionen in diesem Bereich.
Dabei ist zu beachten, dass generative KI-Modelle, die auf Daten aus dem offenen Internet außerhalb Chinas trainiert wurden, von der chinesischen Regierung keine offizielle Lizenz erhalten und daher in einer Grauzone bleiben werden, selbst wenn sie nur intern verwendet werden. Als Ergebnis entwickelt sich in China eine separate generative KI-Industrie, die sich grundlegend vom Rest der Welt unterscheidet.
Die generative KI-Industrie lässt sich in drei verschiedene Wertschöpfungsebenen unterteilen: Infrastruktur, Modelle und Anwendungen. Auf allen diesen Ebenen sind chinesische Firmen aktiv und versuchen, mit den global führenden Firmen in den jeweiligen Segmenten aufzuschließen. So gibt es beispielsweise mit Huawei einen chinesischen Wettbewerber, der auf der Infrastrukturebene Computerchips baut, die für das Training der Modelle genutzt werden sollen. Auf der Modelle-Ebene gibt es eine Vielzahl von Firmen und Universitäten, die eigene generative KI-Modelle trainieren und anbieten. Auf der Anwendungsebene gibt es unzählige chinesische Firmen, die unterschiedlichste KI-basierte B2B- und vor allem B2C-Anwendungen entwickeln.
Trotz fortwährender Fortschritte stehen alle drei Wertschöpfungsebenen in China vor spezifischen Herausforderungen. Auf der Infrastrukturebene gibt es Schwierigkeiten, konkurrenzfähige Computerchips der neuesten Generation herzustellen oder zu erwerben, was größtenteils durch Importverbote aus den USA und deren Verbündeten bedingt ist. Auf der Modelle-Ebene ist der Zugang zu Trainingsdaten oft eingeschränkt, da viele chinesische Daten ausschließlich in mobilen Applikationen oder Super-Apps wie WeChat oder Alipay verfügbar sind, was die Verfügbarkeit von Trainingsdaten reduziert, da diese nicht im offenen Internet zu finden sind. Auf der Anwendungsebene werden umfangreiche Sicherheitsmechanismen und Kontrolltools regulatorisch vorgeschrieben, um die Erzeugung „schädlicher“ und illegaler Inhalte zu minimieren, was die Markteinführung von Produkten oft verlangsamt.
Die Abspaltung des chinesischen generativen KI-Marktes vom Rest der Welt führt dazu, dass in China tätige internationale Unternehmen sich separat mit dem Thema KI in China beschäftigen müssen. Letztlich werden Unternehmen gedrängt, im chinesischen Markt auch chinesische Technologie zu nutzen, wovon auch unternehmensinterne Software betroffen ist.

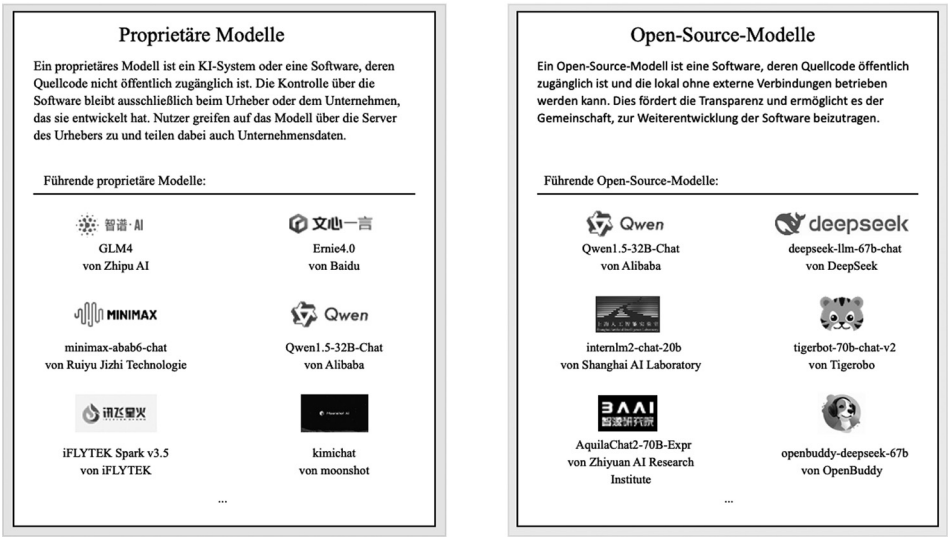
IV. Generative KI-Modelle in China

In den Jahren 2023 und 2024 wurden Hunderte generative KI-Modelle von chinesischen Anbietern entwickelt und veröffentlicht, was zu einem breiten Spektrum an einheimischen generativen KI-Modellen führte. Diese Modelle sind speziell auf die Anforderungen des chinesischen Marktes zugeschnitten und oftmals nur mit Daten in chinesischer und englischer Sprache trainiert. Diese Modelle werden von führenden chinesischen Technologieunternehmen (z. B. Alibaba oder Baidu), Start-ups (z. B. 01.AI oder MiniMax) und Universitäten (z. B. Tsinghua University oder Fudan University) entwickelt.
Unterschiedliche chinesische generative KI-Modelle variieren in Bezug auf die Art des Inputs und Outputs, wodurch verschiedenste Anwendungsfälle möglich werden. Es gibt textbasierte Modelle mit einem Fokus auf Textverarbeitung, spezifische generative KI-Modelle zur Bild- und Videogenerierung oder auch Modelle zur wissenschaftlichen Analyse. In China gibt es zudem den Entwicklungstrend zu multimodalen Modellen, die unterschiedliche Datentypen (Text, Audio, Video, Bilder etc.) sowohl als Input als auch als Output verarbeiten und erzeugen können und dementsprechend flexibel für sehr unterschiedliche Anwendungen eingesetzt werden können. Diese Modelle sind besonders wertvoll für Unternehmen, die eine breite Palette von KI-Anwendungen effektiv integrieren möchten.
Generative KI-Modelle lassen sich auch in China in zwei Gruppen einordnen: Open-Source-Modelle und proprietäre Modelle. Wenn ein generatives KI-Modell als Open-Source-Modell verfügbar ist, kann es von jedem Unternehmen heruntergeladen und auf den eigenen Servern lokal betrieben werden. Hier findet kein externer Datentransfer statt, aber es werden entsprechende Ressourcen wie Serverkosten und IT-Personal für die Bereitstellung und Integration benötigt.
Viele der führenden generativen KI-Modelle in China sind jedoch nur als proprietäre Modelle verfügbar, was bedeutet, dass sie auf der Infrastruktur des Modellentwicklers, wie zum Beispiel Alibaba oder Baidu, laufen und als Datenschnittstellen (API) in eigene Anwendungen integriert werden können. Hierzu ist es jedoch erforderlich, dass der KI-Anwender seine Daten an den Server des KI-Modellanbieters schickt, was zu einem Datenschutzrisiko werden könnte. Auf der anderen Seite werden jedoch keine eigenen teuren und leistungsstarken Server benötigt, die Integration ist sehr einfach und der KI-Modellanbieter rechnet leistungsbasiert auf Grundlage der tatsächlichen Nutzung der generativen KI-Anwendung ab. In der Abbildung (s. ■) sind beispielhaft einige proprietäre und Open-Source-Modelle aufgeführt.

V. Anwendungsfälle Generativer KI in China

Generative KI-Tools sind bereits heute ein fester Bestandteil vieler Unternehmen in China. Sie tragen zur Steigerung der Produktivität bei

Abb.: Generative KI-Modelle in China



und reduzieren gleichzeitig den Personalaufwand. Basierend auf öffentlich bekannten Anwendungen generativer KI von Industrieunternehmen in China geben die Autoren in diesem Kapitel eine Übersicht über die fünf Hauptkategorien der Anwendungsfälle von KI-Tools.

1. Wissens- und Compliance-Management

Generative KI-Systeme erleichtern das Wissensmanagement. Diese Anwendungen, häufig in Form von KI-gestützten Chatbots, haben Zugriff auf ausgewählte unternehmensinterne Daten und ermöglichen es Mitarbeitern, durch natürliche Sprache die gesuchten Daten zu finden oder Antworten auf ihre Fragen zu erhalten. Dies verbessert das Wissensmanagement und beschleunigt die Entscheidungsfindung erheblich.

Anwendungen:

- *Unternehmenswissensmanagement Co-Pilot*: In vielen Unternehmen ist Wissen über verschiedene Abteilungen hinweg fragmentiert und schwer zugänglich. Durch einfache Texteingaben können Mitarbeiter komplexe Datenabfragen durchführen und effizient auf benötigte Informationen zugreifen. Das System verbindet sich mit den benötigten Unternehmensdatenbanken und nutzt fortschrittliche Suchalgorithmen, um relevante Dokumente zu finden.
- *Wartungshandbuch-Assistent:* In produzierenden Unternehmen können spezialisierte Chatbots den Wartungs- oder Problembehebungsprozess erheblich vereinfachen. Basierend auf Problembeschreibungen durchsucht der Co-Pilot digitalisierte Wartungshandbücher und bietet schrittweise Anleitungen zur Problemlösung, was Ausfallzeiten von Maschinen reduziert.
- *Compliance-Assistent:* Ein Compliance-Assistent dient als zentrale Informationsquelle für alle Compliance-Fragen. Mitarbeiter erhalten basierend auf internen und externen Vorschriften Antworten zu ihren Compliance-Fragen und werden proaktiv über Änderungen in gesetzlichen Rahmenbedingungen oder unternehmensinternen Vorschriften informiert.

2. Generative AI für Design und Entwicklung

Generative KI-Anwendungen beschleunigen zeitaufwendige manuelle Arbeit im Design- und Entwicklungsprozess neuer Produkte. Beispielsweise können CAD-Design-Elemente durch natürliche Sprache erstellt werden oder die generative KI-Anwendung unterstützt bei der Entwicklung und dem Testen von Hypothesen über das Verhalten neuer Materialien.

Anwendungen:

- *Produktentwicklungs-Assistent:* Generative KI fördert Innovationen in der Produktentwicklung, indem sie aus Daten wie Kundenfeedback, Markttrends und bestehenden Produktdaten neue Produktideen generiert. Prototypen können so schnell und effizient erstellt werden.
- *Industrial Design Co-Pilot:* KI-basierte Chatbots unterstützen Ingenieure bei Designfragen, bieten automatisierte Designvorschläge und bewerten technische Zeichnungen, was die Effizienz im Designprozess steigert. Durch die Integration von KI-basierten Chatbots in CAD-Systeme wird deren Bedienung benutzerfreundlicher.

3. Prozessoptimierung und Qualitätsmanagement

Generative KI-Modelle beschleunigen die Erstellung und Weiterentwicklung digitaler industrieller Prozesse. Sie unterstützen bei industriellen Programmieraufgaben, analysieren Prozessdaten zur Effizienzsteigerung und sagen Qualitätsprobleme voraus. Kontinuierliche Überwachung und Anpassung der Prozesse steigern die Produktionsleistung und senken Betriebskosten.

Anwendungen:

- *Software Development Co-Pilot*: Generative KI kann den Softwareentwicklungsprozess beschleunigen, indem sie Programmiercode und Dokumentationen automatisch generiert. Besonders nützlich ist diese Technologie bei der Fehlerbehebung und Optimierung komplexer Programmiercodes für PLCs, CNCs oder Robotikanwendungen.
- *Visuelles Qualitätsmanagement-Assistent:* Visuell basierte generative KI-Modelle klassifizieren neue Bilder anhand weniger visueller Beispieldaten und sind so in der Lage, visuelle Inspektionen durchzuführen, um Defekte in den Produkten zu identifizieren.

4. Datenmanagement und -analyse

Generative KI-Modelle können große Mengen an strukturierten und unstrukturierten Daten schnell und zielsicher auswerten. So können

Unternehmensdaten automatisch digitalisiert und tiefere sowie schnellere Erkenntnisse durch Analysen gewonnen werden. Auch können so synthetische Daten erstellt werden, die zur Verbesserung anderer Softwaremodelle genutzt werden können.
Anwendungen:
- *Dokumentenverarbeitung und -digitalisierung Tool:* Generative KI kann unstrukturierte Dokumente effizient verarbeiten und standardisieren, um sie in IT-Systeme zu integrieren. Im Vergleich zu herkömmlichen OCR-Technologien kommt generative KI mit einer Vielzahl von Dokumentenstrukturen und Eingabefehlern klar.
- *Automatisierte Dokumentenerstellung Tool:* KI-Modelle erstellen regelmäßig benötigte Dokumente wie Berichte und Zulassungsdokumente automatisch, indem sie relevante Informationen aus definierten Datenquellen extrahieren, standardisieren und selbstständig in Dokumentenvorlagen einfügen.
- *Data Analyse Co-Pilot:* Generative KI-Modelle analysieren komplexe Datensätze, um wertvolle Erkenntnisse zu gewinnen. Mitarbeiter können durch einfache Chat-Nachrichten Anomalien analysieren und Unternehmenskennzahlen auswerten, was schnellere, fundierte Entscheidungen ermöglicht.

5. Kundeninteraktion und -unterstützung

Generative KI revolutioniert die Kundeninteraktion. Generative KI-gestützte Systeme verbessern die Kundeninteraktion vom Verkaufsprozess bis zum After-Sales-Service, indem sie beispielsweise Kundenanfragen sofort beantworten oder Marketing- und Vertriebsdokumente automatisch erstellen. CRM-Systeme werden automatisch aktualisiert und stets auf dem neuesten Stand gehalten. Diese Technologien erhöhen die Kundenzufriedenheit und steigern die Effizienz der Vertriebsmitarbeiter erheblich.
Anwendungen:
- *Kundenservice-Chatbot:* Generative KI-Modelle beantworten Kundenanfragen automatisiert. Die KI prüft Unternehmensrichtlinien oder Vorschriften und liefert entsprechende Antworten, wodurch die Effizienz des Kundenservices verbessert wird.
- *Marketing- und Vertriebsmaterialien Co-Pilot:* Generative KI ermöglicht die automatisierte Erstellung personalisierter Kundenansprachen und Marketingmaterialien. Von zielgerichteten E-Mail-Kampagnen bis hin zu dynamischen Webinhalten übernimmt die KI einen Großteil der manuellen Arbeit.
- *Lead-Generierung und -Qualifizierung-Tool:* KI-basierte Anwendungen identifizieren und qualifizieren automatisch neue Verkaufsleads aus verschiedenen Online-Quellen, so dass Vertriebsmitarbeiter sich auf das Verkaufen konzentrieren können.

Bei allen vorgestellten Anwendungsfällen stellt sich die Frage, ob internationale Unternehmen Software-as-a-Service (SaaS)-Lizenzen von Anbietern erwerben und diese über das Internet nutzen können, oder ob sie generative KI-Anwendungen spezifisch an ihre eigenen Bedürfnisse anpassen und in ihrer eigenen Infrastruktur betreiben sollten. In China erfüllen viele Anwendungsfälle die qualitativen und sicherheitsrelevanten Anforderungen nur, wenn sie in der eigenen Infrastruktur und somit unter eigener Kontrolle laufen.
Daher ist es ratsam, bei der Anpassung und Implementierung von generativen KI-Anwendungen mit erfahrenen Softwareentwicklungsunternehmen zusammenzuarbeiten oder die erforderlichen technischen Fähigkeiten selbst intern nach und nach aufzubauen. Solche Partnerschaften kombinieren technologische Fähigkeiten mit branchenspezifischem Wissen, um sichere, integrierte und hochqualitative generative KI-Anwendungen zu garantieren.

VI. Überblick über die aktuelle KI-Regulierung in China

China hat sich in den letzten Jahren nicht nur als Vorreiter bei der KI-Entwicklung, sondern auch bei deren Regulierung erwiesen und hat einen grundlegenden Rechtsrahmen für die Entwicklung und Regulierung von KI geschaffen.
Chinas Rechtsrahmen für die Regulierung von KI ist eine Mischung aus politischen Zielsetzungen, Gesetzen, Verordnungen, Richtlinien und Standards. Gemeinsam zielen sie darauf ab, KI-Innovation sowie die Entwicklung und Nutzung von KI-Technologien zu fördern und gleichzeitig die nationale Sicherheit, die Einhaltung ethischer Standards und gesellschaftlicher Werte der VR China zu gewährleisten sowie Verantwortung und Transparenz zu schaffen.
Bereits 2015 hat die chinesische Regierung die KI-Regulierung zu einer Priorität erklärt. KI wurde im Industrieplan „Made in China 2025“ von 2015 als Schlüsselindustrie genannt und im „Next Generation Artificial Intelligence Development Plan“ von 2017 wurde das Ziel festgelegt, bis 2030 weltweit führend und zum wichtigsten KI-Innovationszentrum der Welt zu werden.
Nach der Phase der strategischen Planung und industriellen Selbstregulierung trat China im Jahr 2020 in die Phase der regulatorischen Aufsicht und der Formulierung von freiwilligen Standards. 2020 wurden die „Leitlinien für den Aufbau des nationalen KI-Normungssystems der neuen Generation“ veröffentlicht, in denen acht strukturelle Aspekte des KI-Normungssystems für die Entwicklung technischer Normen durch technische Ausschüsse (TC260) festgelegt sind. 2021 wurden die „ethischen Normen für künstliche Intelligenz der neuen Generation“ erlassen, die u.a. allgemeinen ethischen Prinzipien für die Entwicklung, Lieferung, Verwendung von KI enthalten.
Mit der Festlegung der für die Regulierung von KI notwendigen Datenschutzgesetze im Jahr 2022 hat in China die Phase der direkten sektorspezifischen KI-Regulierung begonnen. Zwei wichtige Meilensteine in dieser Phase sind die „Bestimmungen über Empfehlungsalgorithmen in internetbasierten Informationsdiensten“ und die „Bestimmungen über Tiefensynthese für Internet-Informationsdienste“, die am 1.3.2023 bzw. am 10.1.2023 in Kraft getreten sind. Ziel der beiden Bestimmungen ist es, die ungerechtfertigte Nutzung von Algorithmus-Empfehlungstechnologien wie die „diskriminierende Preisgestaltung durch Big Data“ und die Verwendung von generativer KI zur Erstellung von „Deepfakes“ zu regulieren.
Am 15.8.2023 sind die „Interimsmaßnahmen für das Management von generativer KI“ („KI-Maßnahmen“) in Kraft getreten, die klare Anforderungen an Dienstleister enthalten, die „der Öffentlichkeit in China generative KI-Dienste zur Erzeugung von Text-, Bild-, Audio- oder Videoinhalten anbieten“ („öffentliche KI-Dienstanbieter“).
Neben der Pflicht zur Durchführung einer Sicherheitsbewertung, der behördlichen Registrierung von Algorithmen und anderer Pflichten müssen KI-Dienstanbieter in bestimmten Fällen behördliche Lizenz vom Ministerium für Industrie und Informationstechnologie (MIIT) einholen, bevor sie ihre KI-Dienste der Öffentlichkeit in China anbieten. Die KI-Maßnahmen gelten sowohl für inländische als auch ausländische öffentliche KI-Dienstanbieter.
Bis zum Ende des ersten Quartals 2024 wurden 117 in China entwickelte KI-Modelle für die öffentliche Nutzung zugelassen, jedoch noch kein im Ausland entwickeltes KI-Modell. Auch chinesische KI-Dienstanbieter, deren KI-Produkte auf ausländischen KI-Modellen gebaut sind und die ihre KI-Produkte und -Dienstleistungen der

Öffentlichkeit in China anbieten, fallen in den Anwendungsbereich der KI-Maßnahmen und müssen die Lizenzanforderung sowie andere Pflichten erfüllen.

Die aktuell geltenden KI-spezifischen Regelungen, einschließlich der KI-Maßnahmen zielen primär auf öffentliche KI-Dienstanbieter ab. Die KI-Maßnahmen gelten nicht für Unternehmen, die generative KI-Technologien erforschen, entwickeln oder für interne Zwecke verwenden. Sollte jedoch ein Unternehmen ein KI-Modell für externe Zwecke verwenden, wie z. B. im B2C-Bereich für Kundenchatbots, besteht damit das Risiko, dass das Unternehmen in den Anwendungsbereich der KI-Maßnahmen fällt und entsprechend die Pflichten eines KI-Dienstanbieters erfüllen muss.

Es ist zu erwarten, dass zeitnah weitere verfeinerte KI-Regelungen erlassen werden, einschließlich – wie dem Gesetzgebungsplan des Staatsrates von 2023[2] zu entnehmen ist – eines allgemeinen KI-Gesetzes und auch 50 weitere nationale und industrielle KI-Standards, die bis 2026 erlassen werden sollen.[3]

Auch wenn Unternehmen, die KI-Modelle nur intern einsetzen, nicht in den Anwendungsbereich der vorstehenden Regelungen fallen, so sind bei der Verwendung von KI-Modellen andere, nicht KI-spezifische Rechtsvorschiften zu beachten. Dazu gehören beispielsweise Gesetze und Vorschriften in den Bereichen Datenschutz und Datensicherheit, Produkthaftung, Schutz des geistigen Eigentums, Verbraucherschutz und Werberegelungen.

VII. Rechtliche Herausforderungen bei Verwendung von generativen KI-Modellen in China

Generative KI generiert neben nützlichen Inhalten auch rechtliche Risiken. Diese Risiken reichen vom Verlust von Know-how und der Offenlegung vertraulicher Informationen über Verstöße gegen Datenschutzgesetze, Verletzung von Verbraucherrechten und Diskriminierung bis hin zu Verletzungen von Rechten an geistigem Eigentum und können erhebliche verwaltungs-, zivilrechtliche und strafrechtliche Sanktionen für das die KI anwendende Unternehmen und für deren Geschäftsführung nach sich ziehen.

Diese Risiken drohen nicht nur bei der Verwendung öffentlicher KI-Modelle, wie Chat GPT von Open AI oder Ernie Bot von Baidu, sondern auch nach individueller Anpassung bestehender KI-Modelle auf unternehmensinterne Bedürfnisse und bei deren Einsatz im Unternehmen.

Unternehmen, die generative KI einsetzen oder deren Einsatz planen, sollten daher die rechtlichen Herausforderungen und die daraus resultierenden Risiken identifizieren und, bewerten, damit sie wissen, ob und wie diese reduziert werden können. Nachstehend werden einige der wichtigsten rechtlichen Risiken im Zusammenhang mit dem Einsatz generativer KI-Modelle dargestellt.

1. Urheberrechtliche Herausforderungen

Der Einsatz von generativen KI-Systemen birgt das Risiko, dass die Verwendung der Trainingsdaten bzw. die durch KI-Modelle generierten Inhalte bestehende Urheberrechte Dritter verletzen und gegen das Urheberrechtsgesetz der VR China verstoßen.

Das Risiko besteht insbesondere dann, wenn KI-Basismodelle mit urheberrechtlich geschützten Daten trainiert werden. Die Rechtmäßigkeit der Trainingsdaten beim Input bestimmt die Rechtmäßigkeit der durch das KI-Modell generierten Inhalte beim Output. Wird z. B. ein KI-Modell für Marketingzwecke verwendet, besteht das Risiko, dass die erstellten Marketingmaterialien (Bilder, Videos, Texte usw.) bzw. deren Verwendung Urheberrechte anderer verletzen.

Für die Bestimmung des rechtlichen Risikos ist daher entscheidend, welche Daten für das Training des KI-Basismodells verwendet werden. Da es für Unternehmen praktisch nicht möglich ist, zu überprüfen, mit welchen Daten das KI-Basismodell trainiert wurde, sollten Unternehmen zumindest für die von den KI-Systemen generierten Inhalte zum Zeitpunkt des Outputs prüfen, ob deren Verwendung Urheberrechte anderer verletzt und welche Risiken mit deren Verwendung verbunden sind.

2. Datenschutzrechtliche Herausforderungen

Angesichts der Datenmengen, die zum Training generativer KI-Systeme verwendet werden, ist es oft unvermeidlich, dass diese Trainingsdaten personenbezogene Daten enthalten. Neben den Daten aus dem Internet, die für das Training von KI-Basismodellen verwendet werden, können auch unternehmensinterne Daten, die für die Anpassung des KI-Modells verwendet werden, personenbezogene Daten enthalten.

Darüber hinaus können personenbezogene Daten auch während der Verwendung des KI-Modells eingegeben werden, z. B. in Form einer Frage, eines Fotos oder eines Dokuments. Dies ist typischerweise der Fall, wenn KI-Systeme von Mitarbeitern für Dokumentenverarbeitung oder beim Einsatz von Assistenten in der Personalabteilung und Kunden-Chatbots verwendet werden.

Unternehmen, die mit ihren KI-Modellen personenbezogene Daten verarbeiten, müssen die Einhaltung des Gesetzes der VR China zum Schutz personenbezogener Daten („GSPD“) und anderer einschlägiger Datenschutzvorschriften sicherstellen.

Da die KI-Modelle große Rechenkapazitäten benötigen, werden sie häufig auf Servern von Drittanbietern gehostet. Der Betrieb eigener Server für das Hosting eines KI-Systems ist mit hohen Kosten verbunden und für KMU oft unverhältnismäßig. Werden im Rahmen der Nutzung des KI-Modells personenbezogene Daten auf einem fremden Server gespeichert, kann dies eine Übermittlung personenbezogener Daten an Dritte i. S. v. GSPD darstellen. Unternehmen müssen daher entsprechende Pflichten, insb. Informationspflicht gegenüber dem Betroffenen, erfüllen und eine separate Einwilligung einholen. Weiter empfiehlt sich der Abschluss einer Vereinbarung mit dem KI-Dienstanbieter bzw. dem Serveranbieter über die datenschutzrechtlichen Pflichten und Haftung.

Rechtlich relevant bei der Pflichten- und Haftungsfrage ist der Standort des Servers, auf denen das KI-Modell gehostet wird. Sollte das KI-Modell auf einem Server außerhalb der VR China gehostet werden, liegt bei der Nutzung des KI-Modells durch das Unternehmen in China eine grenzüberschreitende Datenübermittlung vor. Diese ist mit zusätzlichen Datenschutzanforderungen, wie der Einholung einer separaten Einwilligung des Betroffenen, der Durchführung einer Datenschutzfolgenabschätzung usw., verbunden.[4] Dies gilt insbesondere beim Einsatz von ausländischen proprietären KI-Modellen, wie z. B.

2 Gesetzgebungsplan des Staatsrates von 2023: https://www.gov.cn/zhengce/content/202306/content_6884925.htm.

3 Leitlinien für den Aufbau eines umfassenden Normungssystems für die nationale Industrie der künstlichen Intelligenz von 2024: https://www.gov.cn/zhengce/zhengceku/202407/P020240702716282797987.pdf.

4 Mehr Informationen zur grenzüberschreitenden Datenübermittlung *Burkardt/Zapletal*, cross-border data transfer, https://bktlegal.com/files/global/Nachrichten/20221025_BKT_Artikel_TICKER%20WINTER2022_Extrakt.pdf.

ChatGPT, Claude oder Gemini, die oft auf der IT-Infrastruktur außerhalb Chinas laufen.
Unternehmen sollten die datenschutzrechtlichen Risiken durch Datenselektion und Anonymisierung oder andere Maßnahmen reduzieren und soweit möglich sicherstellen, dass keine personenbezogenen Daten in das KI-Modell eingegeben oder hochgeladen werden.

3. Schutz von Geschäftsgeheimnissen und sensiblen Unternehmensdaten

Beim Einsatz von KI-Modellen droht die Offenlegung von sensiblen unternehmensinternen Daten und der Abfluss von Know-how. Das Risiko ist insbesondere bei KI-Modellen für Produktdesign und -entwicklung, Datenmanagement und Prozessoptimierung hoch.
Nach dem Gesetz der VR China gegen unlauteren Wettbewerb werden offengelegte bzw. öffentlich zugänglich gemachte Daten grundsätzlich nicht länger als Geschäftsgeheimnis anerkannt und verlieren damit den entsprechenden Rechtsschutz.
Sollten Unternehmen Geschäftsgeheimnisse oder vertrauliche Unternehmensdaten anderer, wie von Geschäftspartnern, Zulieferern oder Kunden offenlegen oder Dritten zugänglich machen, droht dem Unternehmen außerdem eine vertragliche und gesetzliche Haftung auf Schadenersatz wegen der Verletzung der Geheimhaltungspflichten.
Die Offenlegung der Daten droht nicht nur bei der Verwendung von öffentlichen KI-Modellen (wie ChatGPT), in dem bspw. Mitarbeiter Daten in das KI-Modell eingeben, um eine bestimmte Frage zu beantworten oder ein Dokument zu verfassen bzw. zu übersetzen, sondern auch bei der Verwendung von KI-Modellen, die für interne Zwecke angepasst werden, z. B. indem die entsprechenden Daten dem KI-Anbieter zur Verfügung gestellt werden.
Das Risiko der Offenlegung von Geschäftsgeheimnissen und sensiblen Unternehmensdaten wird erhöht, wenn der Vertrag mit dem KI-Anbieter keinen oder nur einen unzureichenden Schutz vorsieht, bzw. wenn die Nutzungsbedingungen dem KI-Anbieter weitreichende Rechte zur Nutzung solcher Daten einräumen.

4. Verbraucherschutz und Werbung-Compliance

KI-Modelle im Bereich der Kundeninteraktion und -unterstützung können das Marketing, den Vertrieb und den Kundenservice effizienter gestalten und automatisieren. Damit sind jedoch auch rechtliche Risiken verbunden, beispielsweise beim Einsatz von KI-Chatbots im Kundenservice, wenn der Chatbot dem Verbraucher falsche oder irreführende Informationen über das Produkt oder die Dienstleistung erteilt. Dies kann einen Verstoß gegen das Gesetz der VR China zum Schutz der Rechte und Interessen der Verbraucher darstellen und zu Bußgeldern und Schadenersatzansprüchen führen.
Unrichtige oder ungenaue Antworten können verschiedene Ursachen haben. Selbst wenn alle Trainingsdaten richtig sind, kann es bei generativen KI-Modellen zu sog. „Halluzinationen“ kommen, da sie keine deterministischen Modelle sind und nur die wahrscheinlichste Antwort generieren. KI-Anbieter übernehmen daher oft keine Haftung für die Richtigkeit der Outputs ihrer KI-Modelle. Ungenaue Antworten werden beim Testen der KI-Modelle oft übersehen, wenn die Antworten überzeugend und glaubwürdig erscheinen.
Die durch das KI-Modell erstellten Marketingunterlagen müssen ebenfalls den gesetzlichen Anforderungen entsprechen. Wenn Werbeunterlagen falsche oder irreführende Inhalte enthalten, die Verbraucher täuschen, kann dies einen Verstoß gegen das Werbegesetz der VR China und das Gesetz der VR China gegen unlauteren Wettbewerb darstellen.
Um die Genauigkeit des KI-Modells zu erhöhen, sollten Unternehmen alle Quelldaten, die dem KI-Modell bei der Optimierung für den internen Gebrauch zugrunde liegen, auf ihre Richtigkeit überprüfen und regelmäßig aktualisieren sowie die von dem KI-Modell generierten Marketingunterlagen auf Rechtskonformität prüfen. Bei Kunden-Chatbots können Risiken durch eine menschliche Überprüfung der generierten Antworten oder durch eine automatische Weiterleitung an den menschlichen Kundendienst bei technischen oder sensitiven Fragen bezüglich des Produkts verringert werden.
Neben den oben genannten Risiken birgt die Nutzung von generativen KI-Modellen eine Reihe von weiteren Risiken in Bereichen wie Persönlichkeitsschutz, Cybersicherheit, Produkthaftung, Diskriminierung, Marken-, Design- und Patentschutz und Lizenz-Compliance.
Werden KI-Systeme im HR-Bereich bei der Rekrutierung von Mitarbeitern eingesetzt, in dem bspw. der Rekrutierungsprozess durch das Aufnehmen, Bewerten und Aussortieren von Bewerbern durch das KI-Modell automatisiert wird, muss sichergestellt werden, dass keine diskriminierenden Entscheidungen getroffen werden oder Verstöße gegen das Arbeitsgesetz der VR China vorliegen, auf deren Basis Mitarbeiter bzw. Bewerber das Unternehmen auf Schadenersatz und Schmerzensgeld verklagen könnten.
Beim Einsatz von KI-Modellen im Qualitätsmanagement oder Produktdesign können sich die generierten Ergebnisse auf die Produktsicherheit oder -qualität auswirken und Unternehmen müssen daher mit produkthaftungsrechtlichen Risiken rechnen.
Darüber hinaus besteht das Risiko, dass Unternehmen für Verstöße gegen die Lizenz- oder Nutzungsbedingungen des KI-Modells haftbar gemacht werden, denn die Nutzung eines (auch wenn individuell angepassten) KI-Modells sowie der Trainingsdatensätze kann, je nach den spezifischen Nutzungsbedingungen mit unterschiedlichen Verpflichtungen verbunden sein.
Schadenshöhe und Eintrittswahrscheinlichkeit der vorstehenden Risiken variieren je nach dem konkret eingesetzten KI-Modell und dessen Verwendung im Unternehmen.

VIII. Fazit

Anstatt sich von den rechtlichen Herausforderungen, die der Einsatz von generativen KI-Modellen im Unternehmen mit sich bringt, abschrecken zu lassen, sollten Unternehmen die aktuelle KI-Gesetzgebung analysieren (oder von Experten analysieren lassen), darauf basierend die KI-bezogenen Herausforderungen und Risiken identifizieren und bewerten sowie geeignete technische und rechtliche Lösungen suchen, um die Eintrittswahrscheinlichkeit der Risiken bei der Implementierung von generativer KI in ihrem Unternehmen zu mindern.
Auch wenn viele der bestehenden und KI-spezifischen Vorschriften Unternehmen, die KI-Lösungen im Betrieb einsetzen, nicht direkt betreffen, müssen Unternehmen beim Einsatz von KI-Lösungen die Anforderungen der allgemeinen Gesetze erfüllen und insbesondere darauf achten, welches KI-Modell sie wählen, wo es gehostet wird und welche Daten dem KI-Modell zur Verfügung gestellt bzw. in das Modell eingegeben werden. Unternehmen sollten auf jeden Fall verhindern, dass vertrauliche Informationen oder personenbezogene Daten in öffentliche Modelle (wie ChatGPT oder Ernie Bot) eingegeben werden. Weiter ist eine Bewertung der Inhaltssicherheit empfohlen, bei der geprüft wird, ob das Modell „schädliche“ oder falsche Inhalte erzeugt.

Um das Risiko von Bußgeldern, zivilrechtlicher oder strafrechtlicher Haftung zu reduzieren, sollten Unternehmen ihre (Lizenz-)Verträge mit dem KI-Anbieter prüfen (lassen) und, soweit möglich, anpassen.
(Lizenz-)Verträge sollten u. a. klare Nutzungsbedingungen für das KI-Modell, Pflichten beider Parteien und Haftungsklauseln enthalten, insb. die Garantie des KI- Anbieters für die Richtigkeit und Rechtskonformität der Trainingsdaten und der generierten Inhalte, eine Definition von „Geschäftsgeheimnissen" und strenge Geheimhaltungspflichten des KI-Anbieters, wenn Unternehmensdaten für die Anpassung oder Nutzung des KI-Modells verwendet oder in das KI-Modell eingegeben werden.
Unternehmen sollten Regeln für den Umgang mit KI formulieren und diese in unternehmensinterne Mitarbeiterhandbücher aufnehmen sowie Schulungen für Mitarbeiter zur Erhöhung des Risikobewusstseins organisieren.
Es empfiehlt sich weiterhin, eine entsprechende Versicherung abzuschließen, um Haftungsansprüche von Dritten abzudecken, die durch den Einsatz eines KI-Modells entstehen können, da allgemeine D&O- und Betriebshaftpflichtversicherungen diese in der Regel nicht beinhalten.
Selbst wenn die oben genannten Risiken durch rechtliche, technische und organisatorische Maßnahmen verringert werden können, sollten Unternehmen KI-Modelle als ein risikobehaftetes Instrument betrachten und KI-Modelle nur mit Unterstützung von Experten auswählen und im Unternehmen einsetzen.

AUTOREN

Ondřej Zapletal *ist Rechtsberater bei der Anwaltskanzlei Burkardt & Partner in Shanghai. Er hat an der Shanghaier East China University of Political Science and Law chinesisches Bürger- und Handelsrecht studiert und berät ausländische Unternehmen bei deren Investitionen und Geschäften in der VR China. Sein Schwerpunkt liegt auf chinesischem Handels- und Datenschutzrecht.*

Lukas Tatge *ist ein erfahrener Unternehmensgründer und aktuell Mitbegründer sowie CEO des Technologieunternehmens LongAI in Shanghai. LongAI spezialisiert sich auf generative KI-Technologien und bietet eine Vielzahl von Dienstleistungen und Produkten für europäische KMUs in China an. Lukas Tatge verfügt über zwei Masterabschlüsse von der Universität Nanjing und der Universität Göttingen.*